FORTINET
High Performance Network Security

FortiGate-7000 Series Release Notes

VERSION v5.4.5 Build 6481

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

December 20, 2017

FortiGate-7000 v5.4.5 build 6481 Release Notes

01-545-452473-20171220

TABLE OF CONTENTS

Change Log

Date	Change Description
December 20, 2017	Initial version.

Introduction

This document provides the following information for FortiGate-7000 v5.4.5 build 6481:

Supported Models

FortiGate-7000 v5.4.5 build 6481 supports all ForGate-7030E, 7040E, and 7060E models and configurations.

What's New in FortiGate-7000 v5.4.5 build 6481

The following new features have been added to FortiGate-7000 v5.4.5 build 6481 firmware:

M1 and M2 interfaces can use different VLANs for heartbeat traffic (408386)

The M1 and M2 interfaces can be configured to use different VLANs for HA heartbeat traffic.

The following command now configures the VLAN used by the M1 interface (default 999):

```
config system ha
   set hbdev-vlan-id 999
end
```

The following new command configures the VLAN used by the M2 interface (default 1999):

```
config system ha
   set hbdev-second-vlan-id 1999
end
```

GTP load balancing

GTP load balancing is supported for FortiGate-7000 configurations licensed for FortiOS Carrier. You can use the following command to enable GTP load balancing. This command is only available after you have licensed the FortiGate-7000 for FortiOS Carrier.

```
config load-balance setting
   set gtp-load-balance enable
end
```

FSSO user authentication is synchronized

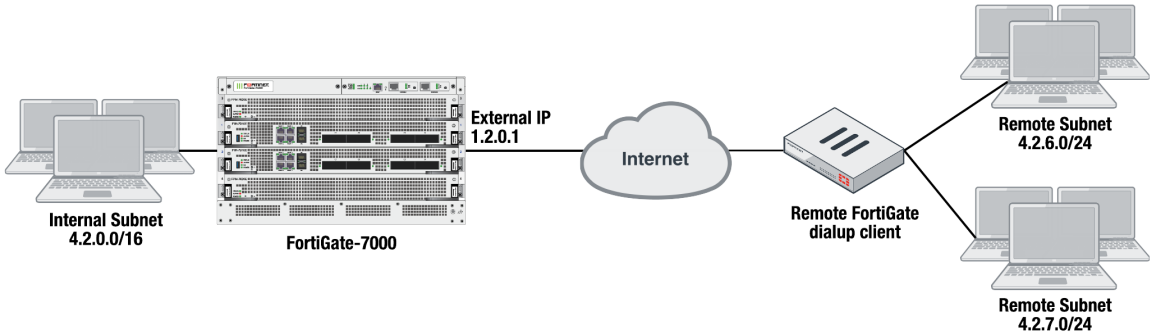
FSSO user authentication is synchronized to all FIM and FPM modules. FSSO users are no longer required to re-authenticate when sessions are processed by a different FIM or FPM module.

HA Link failure threshold changes (422264)

The link failure threshold is now determined based on the all FIM modules in a chassis. This means that the chassis with the fewest active links will become the backup chassis.

FortiGate-7000s running FortiOS v5.4.5 can be configured as dialup IPsec VPN servers

The following shows how to setup a dialup IPsec VPN configuration where the FortiGate-7000 running v5.4.5 acts as a dialup IPsec VPN server.



Configure the phase1, set type to dynamic.

```
config vpn ipsec phase1-interface
   edit dialup-server
      set type dynamic
      set interface "v0020"
      set peertype any
      set psksecret < password>
   end
```

Configure the phase 2, to support dialup IPsec VPN, set the destination subnet to 0.0.0.0 0.0.0.0.

```
config vpn ipsec phase2-interface
   edit dialup-server
      set phase1name dialup-server
      set src-subnet 4.2.0.0 255.255.0.0
      set dst-subnet 0.0.0.0 0.0.0.0
   end
```

To configure the remote FortiGate as a dialup IPsec VPN client

The dialup IPsec VPN client should advertise its local subnet(s) using the phase 2 src-subnet option.

If there are multiple local subnets create a phase 2 for each one. Each phase 2 only advertises one local subnet to the dialup IPsec VPN server. If more than one local subnet is added to the phase 2, only the first one is advertised to the server.

Dialup client configuration:

```
config vpn ipsec phase1-interface
   edit "to-fgt7k"
      set interface "v0020"
      set peertype any
      set remote-gw 1.2.0.1
      set psksecret <password>
   end
config vpn ipsec phase2-interface
   edit "to-fgt7k"
      set phase1name "to-fgt7k"
      set src-subnet 4.2.6.0 255.255.255.0
      set dst-subnet 4.2.0.0 255.255.0.0
   next
   edit "to-fgt7k-2"
      set phase1name "to-fgt7k"
      set src-subnet 4.2.7.0 255.255.255.0
      set dst-subnet 4.2.0.0 255.255.0.0
   end
```

Special Notices

This section highlights some of the operational changes that administrators should be aware of for FortiGate-7000 5.4.5 build 6481.

Recommended configuration for traffic that cannot be load balanced

The following flow rules are recommended to handle common forms of traffic that cannot be load balanced. These flow rules send GPRS (port 2123), SSL VPN, IPv4 and IPv6 IPsec VPN, ICMP and ICMPv6 traffic to the primary (or master) FPM.

The CLI syntax below just shows the configuration changes. All other options are set to their defaults. For example, the flow rule option that controls the FPM slot that sessions are sent to is `forward-slot` and in all cases below `forward-slot` is set to its default setting of `master`. This setting sends matching sessions to the primary (or master) FPM.

```
config load-balance flow-rule
   edit 20
      set status enable
      set ether-type ipv4
      set protocol udp
      set dst-l4port 2123-2123
   next
   edit 21
      set status enable
      set ether-type ip
      set protocol tcp
      set dst-l4port 10443-10443
      set comment "ssl vpn to the primary FPM"
   next
   edit 22
      set status enable
      set ether-type ipv4
      set protocol udp
      set src-l4port 500-500
      set dst-l4port 500-500
      set comment "ipv4 ike"
   next
   edit 23
      set status enable
      set ether-type ipv4
      set protocol udp
      set src-l4port 4500-4500
      set comment "ipv4 ike-natt src"
   next
   edit 24
      set status enable
      set ether-type ipv4
      set protocol udp
      set dst-l4port 4500-4500
      set comment "ipv4 ike-natt dst"
```

```
next
edit 25
   set status enable
   set ether-type ipv4
   set protocol esp
   set comment "ipv4 esp"
next
edit 26
   set status enable
   set ether-type ipv6
   set protocol udp
   set src-l4port 500-500
   set dst-l4port 500-500
   set comment "ipv6 ike"
next
edit 27
   set status enable
   set ether-type ipv6
   set protocol udp
   set src-l4port 4500-4500
   set comment "ipv6 ike-natt src"
next
edit 28
   set status enable
   set ether-type ipv6
   set protocol udp
   set dst-l4port 4500-4500
   set comment "ipv6 ike-natt dst"
next
edit 29
   set status enable
   set ether-type ipv6
   set protocol esp
   set comment "ipv6 esp"
next
edit 30
   set ether-type ipv4
   set protocol icmp
   set comment "icmp"
next
edit 31
   set status enable
   set ether-type ipv6
   set protocol icmpv6
   set comment "icmpv6"
next
edit 32
   set ether-type ipv6
   set protocol 41
end
```

Upgrade Information

FortiGate-7000 v5.4.5 build 6481supports upgrading from FortiGate-7000 v5.4.3 build 6382.

All of the modules in your FortiGate-7000 chassis run the same firmware image. You can upgrade the firmware by using the management IP address to log into the primary interface module GUI or CLI and perform a firmware upgrade just as you would for any FortiGate product. During the upgrade process, the firmware of all of the modules in the chassis upgrades in one step. Firmware upgrades should be done during a quiet time because traffic is briefly interrupted during the upgrade process.

Upgrading an HA configuration

Even if `uninterruptable-upgrade` is enabled, upgrading a FortiGate-7000 HA configuration will cause a minor traffic disruption. You should upgrade HA cluster firmware when traffic is low or during a maintenance period.

IPsec VPN issues when upgrading from v5.4.3 to v5.4.5

If your FortiGate-7000 configuration includes IPsec VPNs you should enhance your IPsec VPN Phase 2 configurations as described in this section. If your FortiGate-7000 does not include IPsec VPNs you can proceed with a normal firmware upgrade.

Because the FortiGate-7000 only allows 16-bit to 32-bit routes for remote subnets, you must add one or more destination subnets to your IPsec VPN phase 2 configuration for FortiGate-7000 v5.4.5 using the following command:

```
config vpn ipsec phase2-interface
   edit "to_fgt2"So
      set phase1name <name>
      set src-subnet <IP> <netmask>
      set dst-subnet <IP> <netmask>
   end
```

Where

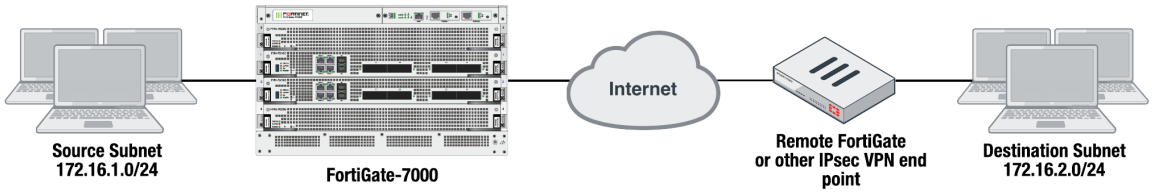
`src-subnet` is the subnet protected by the FortiGate that you are configuring and from which users connect to the destination subnet. Configuring the source subnet is optional but recommended.

`dst-subnet` is the destination subnet behind the remote IPsec VPN endpoint. Configuring the destination subnet is required.

You can add the source and destination subnets either before or after upgrading to v5.4.5 as these settings are compatible with both v5.4.3 and v5.4.5. However, if you make these changes after upgrading, your IPsec VPNs may not work correctly until these configuration changes are made.

Adding source and destination subnets to IPsec VPN phase 2 configurations

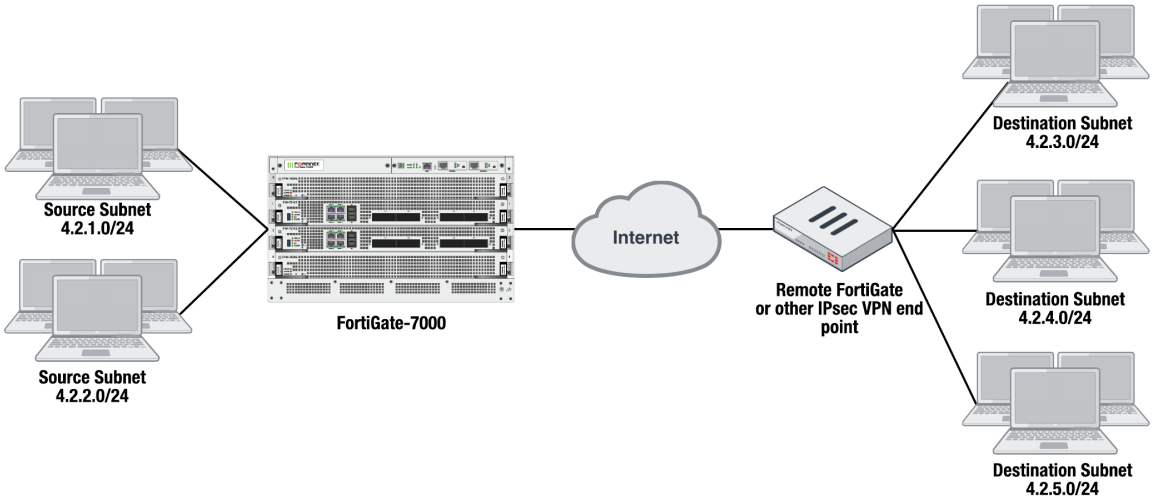
In a simple configuration such as the one below with an IPsec VPN between two remote subnets you can just add the subnets to the phase 2 configuration.



Enter the following command to add the source and destination subnets to the FortiGate-7000 IPsec VPN Phase 2 configuration.

```
config vpn ipsec phase2-interface
   edit "to_fgt2"So
      set phase1name "to_fgt2"
      set src-subnet 172.16.1.0 255.255.255.0
      set dst-subnet 172.16.2.0 255.255.255.0
   end
```

In a more complex configuration, such as the one below with a total of 5 subnets you still need to add all of the subnets to the Phase 2 configuration. In this case you can create a firewall address for each subnet and the addresses to address groups and add the address groups to the Phase 2 configuration.



Enter the following commands to create firewall addresses for each subnet.

```
config firewall address
   edit "local_subnet_1"
      set subnet 4.2.1.0 255.255.255.0
   next
   edit "local_subnet_2"
      set subnet 4.2.2.0 255.255.255.0
```

```
      next
         edit "remote_subnet_3"
      set subnet 4.2.3.0 255.255.255.0
      next
         edit "remote_subnet_4"
      set subnet 4.2.4.0 255.255.255.0
      next
         edit "remote_subnet_5"
      set subnet 4.2.5.0 255.255.255.0
      end
```

And then put the five firewall addresses into two firewall address groups.

```
config firewall addrgrp
   edit "local_group"
      set member "local_subnet_1" "local_subnet_2"
   next
   edit "remote_group"
      set member "remote_subnet_3" "remote_subnet_4" "remote_subnet_5"
end
```

Now, use the firewall address groups in the Phase 2 configuration:

```
config vpn ipsec phase2-interface
   edit "to-fgt2"
      set phase1name "to-fgt2"
      set src-addr-type name
      set dst-addr-type name
      set src-name "local_group"
      set dst-name "remote_group"
   end
```

Product Integration and Support

See the Product Integration and Support section of the FortiOS 5.4.5 release notes for product integration and support information for FortiGate-7000 v5.4.5 build 6481.

Also please note the following exceptions for FortiGate-7000 v5.4.5 build 6481:

Minimum recommended FortiManager firmware version : 5.6.1

Minimum recommended FortiAnalyzer firmware version : 5.4.4

FortiGate-7000 v5.4.5 special features and limitations

FortiGate-7000 v5.4.5 has specific behaviors which may differ from FortiOS features. For more information, see the "Special features and limitations for FortiGate-7000 v5.4.5" section of the most recent version of the FortiGate-7000 Handbook chapter available at http://docs.fortinet.com/d/fortigate-7000.

Resolved Issues

The following issues have been fixed in FortiGate-7000 v5.4.5 build 6481. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
464156	HA heartbeat VLAN tags not correctly applied to HA heartbeat traffic.
464735	Decode VDOM license key failed error messages no longer appear when FortiGate-7000 components start up.
462228	NAT sessions are no longer dropped from DP timers problems after a system restart.
455825	FortiGuard auto-update no longer keeps contacting FortiGuard to request updates after a successful update.
460289	Authenticated users are synchronized to all FPMs. Users no longer have to re-authenticate if some of their traffic is processed by a different FPM.
454070	In an HA configuration, IPv4 routes are now correctly synchronized to all FPMs.
456140	In an HA configuration, only the primary FIM module communicates with FortiManager.
456116	History output of the `diagnose sys ha status` command now includes timestamps to show when failover occurred.
422602	In an HA configuration, failovers no longer occur after an antivirus update.
452415	The output of the `diagnose sys link-monitor status` command is now synchronized.
454411	Local certificates are now synchronized to all FIM modules.
453285	VLAN Traffic continues to flow through Link Aggregation (LAG) interfaces between two FIMs if one of the FIMs is shut down.
448131	Incorrect link local IPv6 addresses that caused IPv6 traffic slowdowns have been corrected.
410647	TCP, HTTP, and UDP-based link monitoring for SD-WAN link load balancing is now supported.
423946	The cmdbsvr process no longer crashes when 500 VDOMs and 10k policies have been configured.
439398	The `diagnose vpn ssl list` command now correctly displays information for all FIM and FPM modules.
442607	Changes to replacement messages made from a VDOM can now be successfully saved.
415234	You can set the **Interface** to **any** when creating a firewall VIP.

Bug ID	Description
410741	AntiVirus, Web Filtering, and other security profile log messages generated by FPM modules now appear on the GUI of all FIM or FPM modules (including the GUI of the primary FIM module).
417584	HA chassis failover from management links only occurs if no management links are available on the chassis. As long as at least one management link is available a failover will not occur.
424015	Fixed a bug with firmware updates with `uninterruptable-upgrade` enabled to cause extra chassis failovers.
408535	The hostname is now synchronized to all modules.
392288	A configuration that includes 500 VDOMs can now be restored from the GUI.

Known Issues

The following issues have been identified in FortiGate-7000 v5.4.5 build 6481. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
449276	FortiGuard IPS signature updates may cause an HA failover.
455632	FIM modules may incorrectly leave and rejoin an HA cluster.
444107	Remote disk share mounting fails when using NFS v2/v3 over UDP. To work around this issue use NFS over TCP.
440550	Some FortiView pages may display Failed to get FortiView data error messages.
460148	The application field in system event log crash messages is unreadable.
459413	HA remote IP monitoring using the `pingserver-monitor-interface`, `pingserver-failover-threshold`, and `pingserver-flip-timeout` options does not work.
459424	The GUI the VDOM list page does not show correct CPS, CPU, and memory usage for each VDOM.
456872	Routes to LACP LAGs are not synchronized to all modules.
442168	Traffic counters that display interface traffic for a physical interface do not display traffic sent and received by VLANs added to the physical interface.
422404	FPMs cannot communicate with the configured FortiAnalyzer if source-ip is set to the IP address of a management interface.
449298	FortiGate-7000 resource utilization is not reported correctly by FortiAnalyzer.

FORTINET®

High Performance Network Security